Formal Methods, Security Models and Implementations

George W. Dinolt
CS4605

Introduction

- The Process
- Policy
- Math Model
- Specification
- Implementation
- Mappings

The Process

- Describe the Security Policy in Words
- Map that Policy into a Mathematical Model
- Build a Formal Top Level System Specification
- Prove that the Specification satisfies the Mathematical Model
- Implement the Specification and run on real hardware
- Determine that the Implementation is a faithful representation of the Specification

Information Flow Policy

- Describe the active Entities in the system
- Describes a security boundary
- Describe which Entites reside "inside" and which "outside"
- Describes what crosses the boundary
- Describe the transitions that can occur (input to generate output)
- Describes Assumptions about the inputs to transitions
- Describes the Assertions to be made about outputs of the transitions

The Math Model

- Set of (undefined) terms that are the "words" of the language
- Definitions that define new words (terms) in terms of the Undefined terms
- Functions that describe potential relationships among the terms and define potential transitions from one set of values to another
- Axioms that are the Assumptions about the input terms
- Theorems that are a consequence of the Axioms and definitions and show properties of the ouputs
- Assumptions and Theorems are properties (relationships) among the terms (assumed and defined)

Policy – Model Mapping

- Undefined terms $\leftrightarrow$ What crosses the boundary between the entities
- Functions and Definitions $\leftrightarrow$ Relationships/connections/transitions among the entities
- Axioms $\leftrightarrow$ Assumptions
- Theorems $\leftrightarrow$ Assertions

Top Level Specification

- Map the Undefined Terms to Types
- Map Definitions to structures (classes, records) of Types
- Map the Functions to Functions on Types in the Specification
- Map the transitions to the "processes" of the the system
- Map the Assumptions into properties that inputs must satisfy
- Map the Theorems to properties guaranteed about the outputs

Simple Notation

- $\mathcal{P}(X) = 2^X = \{A : A \subseteq X\} =$ powerset of X
- $< x_1, x_2, x_3, \ldots, x_n, \ldots >$ a sequence of elements
- $< x : x \in X >$ is the set of all sequences of elements of X
- $\wedge$ is and
- $\vee$ is or
- $\ni$ is such that
- $X \times Y = \{(x, y) : x \in X \wedge y \in Y\}$ is the cross product of X and Y

Examples - Trivial System*

- Undefined Terms are
  - $\mathcal{IU}$ and $\mathcal{LABEL}$
- Defined Terms are
  - $Streams = \{st : st =< iu,\ iu \in \mathcal{IU} >\}$
  - $Networks = \mathcal{LABEL} \times Streams$
  - $Systems = \mathcal{P}(Networks) \times \mathcal{P}(Networks)$
  - $ExactMatchSystems = \{(INets, ONets) \in Systems :$
    $\forall (olb, ostr) \in ONets,\ \forall iu \in ostr\ \exists (ilb, istr) \in INets \ni$
    $iu \in istr\ \wedge\ ilb = olb\}$

*See first Lecture

Interesting Theorem

Suppose $(INs, ONs) \in Systems$. Suppose we assume that $\forall iu$ if

$$iu \in str_1 \wedge ((lb_1, str_1) \in INs \vee (lb_1, str_1) \in ONs)$$

and

$$iu \in str_2 \wedge ((lb_1, str_2) \in INs \vee (lb_2, str_2) \in ONs)$$

implies $lb_1 = lb_2$. Then $(INs, ONs) \in ExactMatchSystems$.[†]

[†] This is a complicated way of saying that all the networks in which iu appears have the same label then the system is exact match secure

Potential Problems

- The implementation runs on real hardware
- The running Implementation may not be a faithful representation of the Specification because of:
  - Properties in implementation not faithfully mapped back to model (subverts model in some way not captured in the mapping)
  - Misunderstandings of how the hardware works
  - Faults caused by interactions with the environment
  - Failure of the hardware components

Potential Advantages

- Clear Definition of what system should accomplish
- Can reason about system properties without considering entire system
- Structures the development process
- Provides precise statements of what should be tested - the assertions and assumptions (axioms and theorems)